

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

CIPHERBLADE, LLC, a Pennsylvania Limited  
Liability Corporation

PLAINTIFF,

v.

CIPHERBLADE, LLC, an Alaska Limited Liability  
Corporation, MANUEL KRIZ, MICHAEL  
KRAUSE, JORN HENRIK BERNHARD  
JANSSEN, SERGIO GARCIA, JUSTIN MAILE,  
IOANA VIDRASAN,

and

CIPHERBLADE APAC PTE LTD, a Singapore  
limited company, JUSSI AITTOLA,

and

OMEGA3ZONE GLOBAL LTD, a Cyprus limited  
company, PAUL MARNITZ,

and

INQUISITA SOLUTIONS LTD., a Cyprus limited  
company

and

GREEN STONE BUSINESS ADVISORY FZ LLC,  
a United Arab Emirates Limited Liability  
Corporation.

DEFENDANTS.

**CASE NO. 1:23-CV-05671-AKH**

**JURY TRIAL DEMANDED**

**FIRST AMENDED COMPLAINT**

1. Plaintiff CipherBlade, by and through its attorneys, Crowell & Moring LLP, submit this Amended Complaint against Defendants CipherBlade LLC, an Alaska Limited Liability

Corporation; Manuel Kriz; Michael Krause; Jorn Henrik Bernhard Janssen; Sergio Garcia; Justin Maile; Ioana Vidrasan; CipherBlade APAC PTE LTD, a Singapore limited company; Jussi Aittola; Omega3Zone Global LTD, a Cyprus limited company; Inquisita Solutions Ltd. a Cyprus limited company; and Green Stone Business Advisory FZ LLC, a Dubai company, hereby allege as follows:

### **NATURE OF THE ACTION**

2. This is a civil action for misappropriation of trade secrets under the Defend Trade Secrets Act, 18 U.S.C. § 1836, (ii) the Computer Fraud and Abuse Act (18 U.S.C. § 1030 *et seq.*), (iii) unfair competition (15 U.S.C. § 1125(a)), (iii) related state claim claims for tortious interference with contracts, tortious interference with business advantage, conversion, trespass to chattels, fraud, and unjust enrichment, and (iv) the Racketeer Influenced and Corrupt Organizations Act (18 USC § 1961, *et seq.*).

3. Plaintiff seeks injunctive and other equitable relief and damages against Defendants who wrongfully control and operate Plaintiff CipherBlade's IT infrastructure and converted corporate assets, including customer and business trade secrets and confidential information, and who pass off CipherBlade's services for their own. Defendants, through their illegal activities involving misuse of CipherBlade assets, infrastructure, and resources, have caused and continue to cause irreparable injury to Plaintiff, their customers, and the public.

### **PARTIES**

4. Plaintiff CipherBlade LLC (hereinafter, "CipherBlade PA" or "Plaintiff") is, incorporated in Pennsylvania, owned by Richard Sanders and has a Certified Investigative Partnership with Chainalysis, which operates in New York City, New York.

5. Defendant CipherBlade LLC (hereinafter, "the Alaska Entity") is, on information

and belief, an Alaska limited liability corporation with offices at 310 K Street, Suite 200, Anchorage, AK 99501 and which is owned and/or controlled by Mr. Justin Maile.

6. Defendant CipherBlade APAC PTE LTD (hereinafter, “the Singapore Entity”) is, on information and belief, a Singapore limited company with offices at 30 Cecil Street, #19-08 Prudential Tower, Singapore 049712 and which is owned and/or controlled by Mr. Jussi Aittola.

7. Defendant Omega3Zone Global LTD is, on information and belief, a Cyprus limited company with offices at 9 Stelmio Building, Flat/Office 301, 8020, Paphos, Cyprus, Greece and which is owned and/or controlled by Mr. Paul Marnitz.

8. Defendant Manuel Kriz (also known as “Matthew Greene”) is a natural person domiciled, on information and belief, in Cyprus at 9, Stelmio Building, Floor 3, Flat/Office 301, 8020, Paphos, Cyprus, Greece.

9. Defendant Michael Krause is a natural person domiciled, on information and belief, in Georgiou Pitrou, Mesogi, Paphos, 8280, Cyprus.

10. Defendant Jorn Henrik Bernhard Janssen (also known as “Jan”) is a natural person domiciled, on information and belief, in Cyprus at 9 Stelmio Building, Floor 3, Flat/Office 301, 8020, Paphos, Cyprus, Greece.

11. Defendant Ioana Vidrasan is a natural person domiciled, on information and belief, in Cyprus at 9 Stelmio Building, Floor 3, Flat/Office 301, 8020, Paphos, Cyprus, Greece.

12. Defendant Jussi Aittola is a natural person domiciled, on information and belief, in Singapore.

13. Defendant Justin Maile is a natural person domiciled, on information and belief, in Alaska at 655 W 22nd Ave, Anchorage, AK 99503.

14. Defendant Paul Marnitz is a natural person domiciled, on information and

belief, in Cyprus at 9 Stelmio Building, Floor 3, Flat/Office 301, 8020, Paphos, Cyprus, Greece.

15. Defendant Sergio Garcia is a natural person domiciled, on information and belief, in Belgium.

16. Defendant Inquisita Solutions Ltd. is, on information and belief, a Cyprus limited company with offices at 9 Stelmio Building, Floor 1, Flat/Office 102, 8020, Paphos, Cyprus, Greece.

17. Defendant Green Stone Business Advisory FZ LLC is, on information and belief, a Dubai limited company with offices at A4-712, Building no. A4, Al Hamra Industrial Zone-FZ, Ras Al Khaimah, United Arab Emirates.

### **JURISDICTION AND VENUE**

18. This Court has subject matter jurisdiction over this case pursuant to the Defend Trade Secrets Act (18 U.S.C. § 1836), the Computer Fraud and Abuse Act (18 U.S.C. § 1030 *et seq.*), unfair competition under the Lanham Act (15 U.S.C. § 1125(a)), and the Racketeer Influenced and Corrupt Organizations Act (18 USC § 1961, *et seq.*). The Court also has supplemental jurisdiction for the New York State law claims pursuant to 28 U.S.C. § 1367.

19. This Court also has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, because, upon information and belief, all the Defendants are citizens of jurisdictions other than the states where Plaintiff is a citizen and the amount in controversy exceeds \$75,000.

20. The venue in this action is proper within the Southern District of New York pursuant to 28 U.S.C. § 1391(b) because (i) CipherBlade PA's partner and customers for CipherBlade PA's services are based in New York, which is an important market for cryptocurrency loss investigative and related expert witness services; (ii) the claims asserted by Plaintiff arose within this District, and (iii) there is no district better suited in which this action

may otherwise be brought.

21. Defendants are subject to personal jurisdiction in the State of New York and venue in this Court because through tortious conduct in this District they caused injury to CipherBlade PA's important business partnerships and customer relations with entities based in this District.

22. New York is a critical market for the cryptocurrency investigative, recovery and related expert witness services that CipherBlade PA provides. Indeed, CipherBlade PA provides cryptocurrency investigative and recovery services and expert testifying services to institutions and individuals based in the Southern District of New York, including as examples investigative work for a victim in connection with *SEC v. Elmaani*, 20 Civ. 10374, a case in this District, and investigative and testifying work in connection with *LCX AG v. Doe and \$1.274 M U.S. Dollar Coin*, Index 154644-2022 a case in the New York Supreme Court in New York County. Indeed, CipherBlade PA's work in the last three years has included four engagements to act as an expert in a lawsuit involving cryptocurrency pending in the federal or state courts in New York County and numerous other engagements that did not result in or involve an action in court.

23. CipherBlade PA's relationship with law firms based in this District representing clients involving cryptocurrency losses is a critical source of CipherBlade PA's business. CipherBlade PA is also retained to provide insight in connection with government cryptocurrency enforcement matters that take place in this District. In this capacity, CipherBlade PA interacts with prosecutors and regulators in this District concerning cryptocurrency investigations on behalf of clients, including a cryptocurrency exchange.

24. CipherBlade PA's most important business partner and relationship is with Chainalysis, Inc. ("Chainalysis") which is based in this District, and with which CipherBlade PA

works in connection with investigations in this District and elsewhere. CipherBlade PA also licenses Reactor, a Chainalysis blockchain analysis software and platform, to do this work. CipherBlade PA would be unable to continue in business without maintaining this key relationship. Indeed, the Chainalysis blockchain analysis software and platform is a critical tool, without which CipherBlade PA cannot operate effectively and efficiently.

25. The Chainalysis relationship is also a critical source of new business leads that Defendants have been converted by Defendants. This relationship has been severely compromised as part of Defendant's scheme, and Defendants are actively seeking to lock out Plaintiff from their Chainalysis accounts and all historical data associated with Plaintiff's ongoing investigations, which prevents CipherBlade PA from continuing its operations and threatens to irreparably destroy its operations and reputation.

26. The Defendants interfered with Plaintiff's Chainalysis relationship and agreement by contacting Chainalysis directly, to directly access Reactor and restrict CipherBlade PA's access to a product that is crucial for its day-to-day functions. Defendants sought to change the billable entity of the Chainalysis Reactor account from PA to Alaska.

27. Though Mr. Kriz sent a request to change the CipherBlade PA's contract after he was terminated, Plaintiff still has access to Reactor at this time. The use of Reactor is central to conducting investigations on the blockchain, which is the focus of their entire business.

28. Accordingly, the wrongful acts of Defendants have caused irreparable harm to CipherBlade PA and their crucial client and partner relationships in this District, including by Defendants wrongly passing themselves off as CipherBlade PA and accessing and using the Chainalysis software platform. In so doing, the Defendants accessed and misappropriated confidential information and trade secrets, including information concerning the relationship with

Chainalysis as well as CipherBlade PA client information to falsely conduct business as Plaintiff or as related to or as a successor to Plaintiff.

29. Furthermore, Chainalysis now has reservations about working with CipherBlade PA, due to the perceived instability of the company's personnel and structure, as well the potential for further drama between the Defendants and CipherBlade PA.

## **FACTUAL BACKGROUND**

### **Introduction**

30. In mid-2018, Mr. Richard Sanders co-founded CipherBlade in the United Kingdom as CipherBlade Ltd. (the "UK Entity"). On February 19, 2019, Mr. Sanders created and incorporated the company in the United States as CipherBlade, LLC ("CipherBlade PA"), which is wholly owned by Mr. Sanders. The business contracts, clients, and infrastructure was transferred to CipherBlade PA around late February and early March 2021.

31. CipherBlade PA is a blockchain investigation company that investigates cryptocurrency-related matters, often involving cybercrime. CipherBlade PA also tracks Bitcoin and other cryptocurrency assets. Over the last five years, CipherBlade PA has investigated, tracked and provided consulting services on cases leading to the recovery of over \$50 million, and the location of cryptocurrencies or other assets obtained through cryptocurrency transactions valued in the billions of dollars.

32. CipherBlade PA also assists federal government agencies, private companies, and individuals in investigations of financial crimes. CipherBlade PA has engaged and continues to engage in activities designed to promote its services domestically and overseas. And over the course of its work and promotional activity, CipherBlade PA has developed a reputation in the

industry and with the U.S. government and private entities alike as a trusted partner in these types of investigations and has garnered goodwill throughout the industry.

33. In late 2022, Mr. Sanders sought to take a step back from the day-to-day operations of CipherBlade PA to volunteer in Ukraine assisting the Ukrainian National Police with investigations involving cryptocurrency.

34. As explained herein, after Mr. Sanders left for Ukraine, Defendants engaged in theft of CipherBlade PA trade secrets, theft of property and assets, fraudulent misrepresentations regarding key aspects of the business to Mr. Sanders and third parties and engaged in a criminal racketeering scheme to steal CipherBlade PA, its clients, and its assets away from Mr. Sanders.

35. Specifically, knowing Mr. Sanders would be in Ukraine, prior to and just after his departure, Defendants made material misrepresentations to Mr. Sanders to gain access to his accounts, stole trade secrets in the form of attorney-client documentation, customer leads, customer lists, and investigatory data (including confidential Chainalysis transaction and investigative graph data), and stole access to the CipherBlade PA business itself. The Defendants engaged in mail and wire fraud in furtherance of their scheme by using Mr. Sanders' information to take over the CipherBlade.com Domain, and CipherBlade IT infrastructure. With access to CipherBlade PA's internal systems, Defendants continue to make material misrepresentations that have resulted in interference with contracts and business relationships, loss of client engagement, and have even siphoned off significant funds via fraudulent entities and shell companies.

#### **CipherBlade PA Personnel**

36. In May/June 2019, Manuel Kriz was hired at CipherBlade UK Ltd. to work as an investigator, as well as handle back-office related items such as invoices, business leads, general



company email responses, engagement agreements and other contractual items (generation thereof – not signing), and client calls. Defendant Kriz was also a shareholder of the business.

37. Mr. Kriz was responsible for some finance-related duties and did not have the authority to sign any documents on Mr. Sanders' behalf or make any critical decisions for CipherBlade PA. Mr. Kriz also did not have ownership of CipherBlade PA in any form.

38. In mid-2021 Mr. Kriz told Mr. Sanders that he was hiring an additional individual, Mr. Michael Krause, in a limited capacity, to assist with CipherBlade PA's daily tasks. However, shortly thereafter, in late 2021/early 2022, Mr. Kriz advised Mr. Sanders that he required more assistance with his daily tasks and would be elevating Mr. Krause to a more substantial role.

39. Over time, Mr. Sanders gave Mr. Krause limited authority, upon request, to take on additional backend duties, such as handling routine transactions and routine administrative functions, for which Mr. Sanders would be made aware (e.g., compensating staff, Reactor license payments to Chainalysis, etc.). Mr. Krause was a contractor who, over time, grew into a trusted business colleague and friend to Mr. Sanders.

40. Mr. Krause, as a contractor, never owned any portion of CipherBlade PA and has no equity interest in the company.

41. In late 2022, as Mr. Sanders prepared for his trip to Ukraine, he recognized that he required assistance managing the administrative, business management, and accounting tasks at CipherBlade PA, which he normally oversaw. Mr. Sanders entrusted Mr. Kriz and Mr. Krause with these tasks for several months in preparation for Mr. Sanders' time in Ukraine, starting in February 2023.

42. Both Mr. Kriz and Krause were granted limited administrative access and authority to manage CipherBlade PA's IT infrastructure and were also authorized to retain others as needed.

43. In late 2022/early 2023 Mr. Kriz hired Mr. Krause's two sons, Jorn Henrik Bernhard Janssen and Paul Marnitz, as well as Ioana Vidrasan. These three individuals were hired in an assistant-like capacity.

44. Mr. Kriz and Krause also subsequently hired Justin Maile in March 2023 and Jussi Aittola in April 2023. Both Mr. Maile and Mr. Aittola were former employees of Chainalysis.

45. Paul Sibenik was hired at CipherBlade in 2019. He was the Lead Case Manager and the most senior full-time investigator at the company. He has often been called upon as an expert in cryptocurrency-related investigations and resulting cases.

46. After being hired in 2019, Mr. Sibenik's responsibilities increased over time. Mr. Sanders, Principal and founder of CipherBlade PA, expanded the scope of his work to include overseeing more business and operational tasks.

47. On June 16, 2023, Mr. Sanders transitioned the role of CEO to Mr. Sibenik.

**Defendants Made Material Misrepresentations  
to Mr. Sanders as Part of a Scheme to  
Steal CipherBlade PA, Its Assets, and Trade Secret Information**

48. At a certain point in time, the Defendants represented to Mr. Sanders that setting up separate entities may be necessary to facilitate business opportunities and segregate business lines in the future. Defendants then falsely represented to Mr. Sanders that the separate CipherBlade entities would be set up in Alaska and Singapore and each would be: (i) affiliated with CipherBlade PA, and (ii) registered as owned by Mr. Sanders.

49. The Defendants spent significant time explaining to and attempting to convince Mr. Sanders that this was a necessary part of CipherBlade's logical growth and expansion.

50. While Mr. Sanders consented to Mr. Maile's hiring, it was later discovered that Mr. Maile was not technically employed by CipherBlade PA and had far exceeded the role Mr. Kriz

originally proposed he would fill. Rather, Mr. Maile almost immediately went out on his own and created his own company, mimicking the name “CipherBlade LLC,” and incorporated it in Alaska (“the Alaska Entity”).

51. Similarly, Mr. Aittola also created his own limited company in Singapore, CipherBlade APAC Pte Ltd (“the Singapore Entity”).

52. In truth, neither the Alaska Entity or the Singapore Entity was associated with CipherBlade PA or Mr. Sanders.

53. It was well known among CipherBlade PA staff that Mr. Sanders intended to volunteer his time and services to assist the people in Ukraine for at least a few months in early 2023. Unfortunately, almost immediately after Mr. Sanders departed for Ukraine, Defendants began engaging in a series of activities that were unauthorized and far exceeded the parameters of the authorized scope of their work and permissions.

54. These acts involved fraudulent misrepresentations and conduct by which Defendants conspired to convert CipherBlade PA assets – including its corporate trade secrets and confidential information, employees and contractors, business contracts, customer contracts and financial assets – and to transfer these assets to their control, as well as the control by entities operated by Defendants, all without Mr. Sanders’ authorization.

**Defendants, Through Misrepresentations,  
Gained Access to Mr. Sanders Email and Personal Information,  
Which They Used to Impersonate Mr. Sanders and Engage in Mail and Wire Fraud**

55. Immediately before Mr. Sanders went to Ukraine, he granted the Defendants limited authority to create and utilize the richard@cipherblade.com email address to facilitate electronic signing of routine client engagements alone. While Mr. Sanders was aware of the richard@cipherblade.com email address, he did not have access to its inbox.

56. Mr. Sanders trusted that when his colleagues used this email address for more than the limited purpose described above, they would make him aware of the reasons why and request authorization. Unfortunately, this was not the case.

57. Defendants repeatedly used Mr. Sanders' email and credentials in a fraudulent manner which exceeded their authorization. While Defendants had full access to use "richard@cipherblade.com," Defendants used this email account to fraudulently communicate with others, purportedly on behalf of CipherBlade PA and as Mr. Sanders himself.

58. On multiple occasions, Defendants also tried gaining access to Mr. Sanders' personal "rich@cipherblade.com" email but were unsuccessful. For example, on January 31, 2023, Defendants solicited Mr. Sanders for access to his personal "rich@cipherblade.com" email, which he did not provide. Defendants repeatedly made these types of access requests, messaging Mr. Sanders to ask for direct access to his email to complete administrative tasks. In hindsight, Mr. Sanders believes that their solicitations were part of their larger scheme.

59. For example, on or around April 18, 2023, Mr. Sanders asked that Mr. Krause send a termination notice to Mr. Kriz. Mr. Krause used the "richard@cipherblade.com" email to do so instead of using his own email address, which Mr. Sanders found suspicious. Defendants did not have authority to use the richard@cipherblade.com email address account in this way. Rather, Defendants displayed a pattern of impersonating Mr. Sanders using his name and photo, to fraudulently advance their efforts. *See Figure 1.*

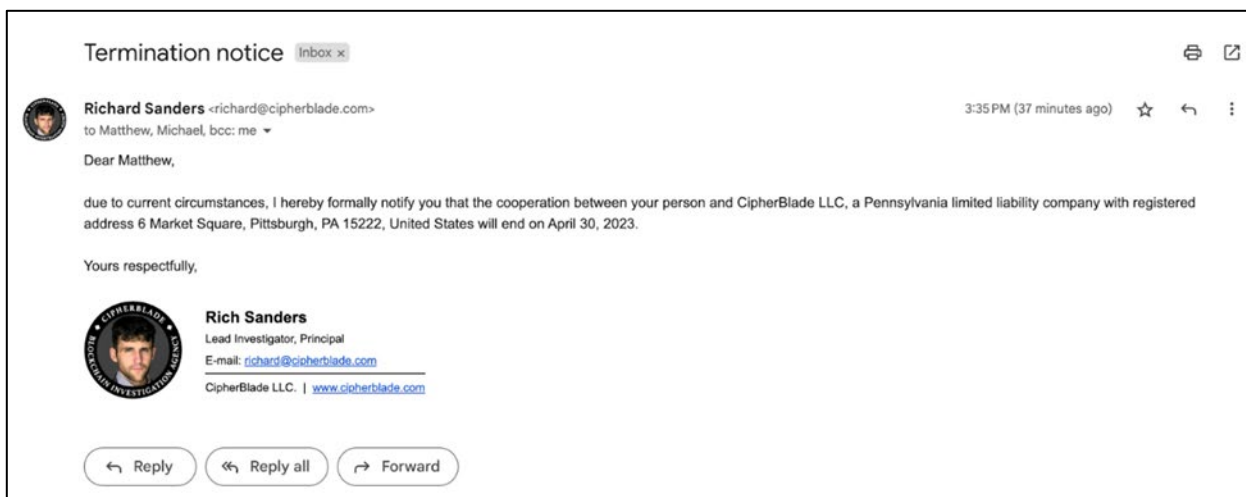


Figure 1

60. Defendant Manuel Kriz regularly went by the alias “Matthew” and Defendant Michael Krause is referred to here as “Michael.”

61. Mr. Kriz’s termination was effective on April 30, 2023.

62. Mr. Sanders immediately messaged Mr. Krause saying, “This is a strange way of handling it, no? Why is only one entity mentioned? And why did it need to come from ‘my’ email, why could it not have been from Michael?” *See Figure 2.*

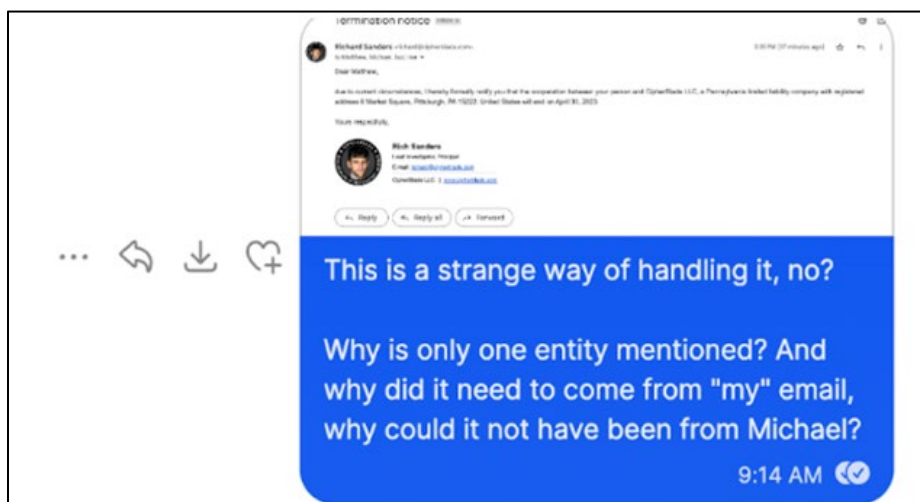
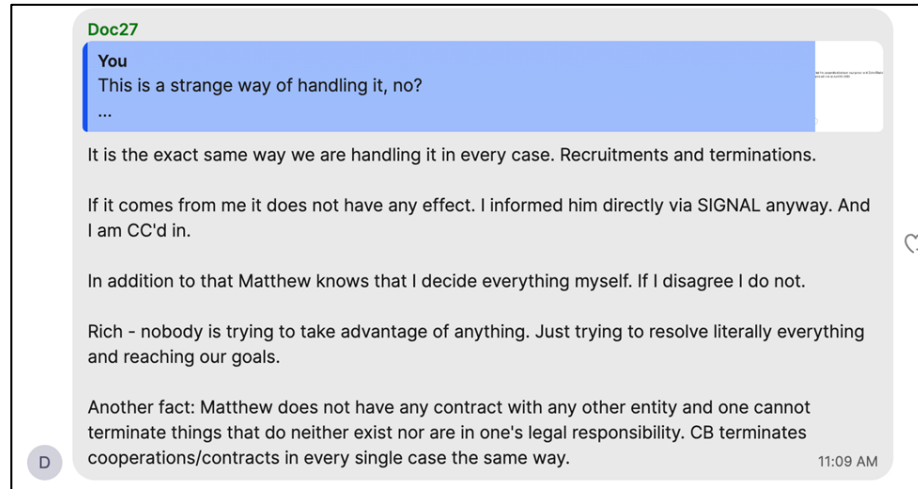


Figure 2

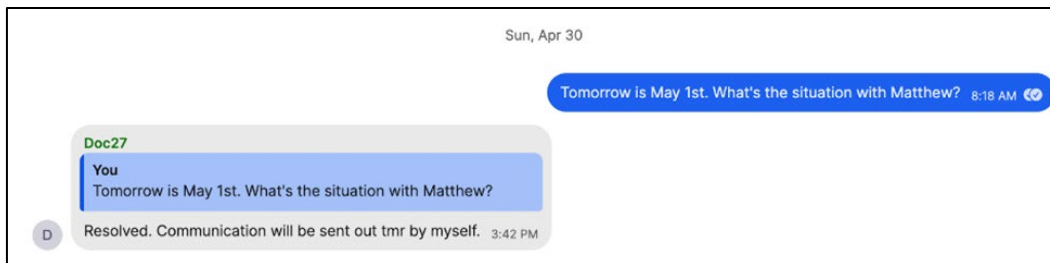
63. Mr. Krause as seen in Figure 3 below using the handle “Doc27” assured Mr. Sanders that no one is trying to take advantage of him and explained that “if it comes from me it does not have any effect.” See **Figure 3**.



**Figure 3** (“Doc27” is Defendant Michael Krause.)

64. On April 30, 2023, Mr. Sanders followed up on the situation with Mr. Kriz, which Mr. Krause explained was “resolved.” We now know that this was untrue. Mr. Kriz had not been terminated. In fact, Mr. Kriz continued to be involved with CipherBlade PA and conspired with Defendants to engage in this scheme. Mr. Sanders learned about this when he saw that Defendant Kriz’s email account, which as part of off boarding should be shut down, was still accessing a CipherBlade PA Google spread sheet.

65. Defendant Kriz was using his CipherBlade PA email to access CipherBlade PA files in their Google drive, after his apparent termination. Defendant Kriz also engaged on CipherBlade PA’s internal channels to chat with other contractors, giving the impression that he was still part of the company. See **Figure 4**.



**Figure 4** (“Doc27” is Defendant Michael Krause.)

66. Defendants also began contacting customers and contractors, purportedly on behalf of Mr. Sanders, but without Mr. Sanders’ knowledge or authorization, and attempting to re-negotiate agreements. These emails went so far as to include a *picture* of Mr. Sanders on the signature line.

67. For example, on March 29, 2023, Defendants accessed Mr. Sanders email and terminated an existing contractor agreement with Mr. Sibenik with CipherBlade PA in order to change a previously agreed upon revenue sharing structure. Defendants sought to represent this communication as coming from Mr. Sanders. This document was not from Mr. Sanders, nor was Mr. Sanders aware that the Defendants emailed such an agreement to Mr. Sibenik. Defendant Mr. Krause’s email is copied in the communication below. *See Figure 5.*

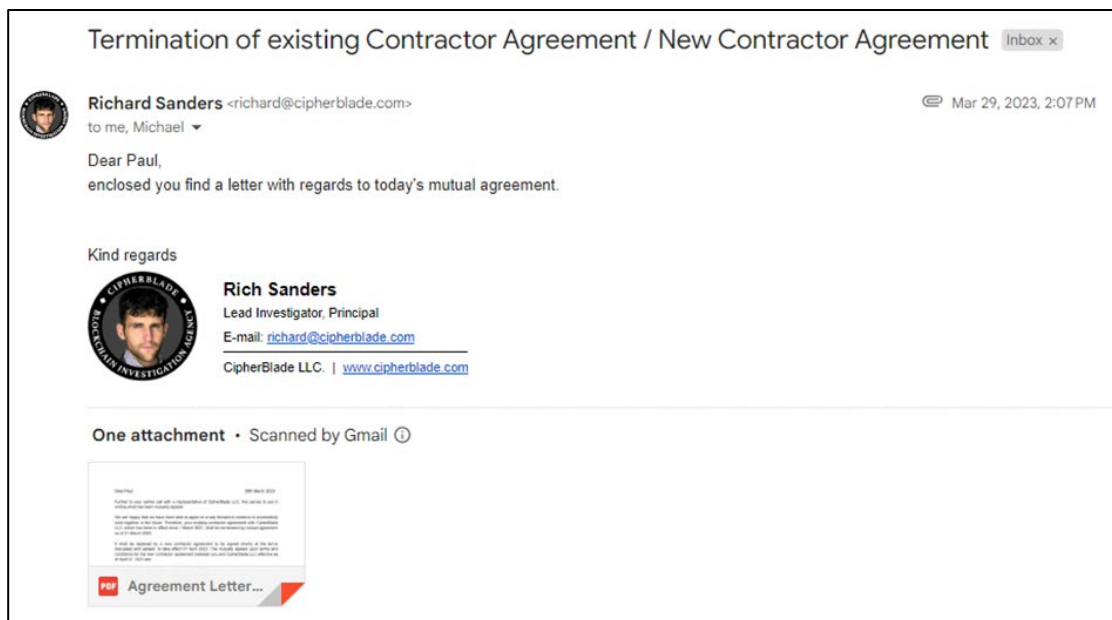


Figure 5

68. The Defendants also engaged in physical theft and impersonation outside of the digital world, by engaging in theft of business documents, credit card fraud, and impersonating Mr. Sanders via federal mail.

69. On at least one occasion, while abroad in Ukraine, Mr. Sanders received a series of alerts from his home security system that indicated all of his security cameras suddenly went offline. Upon returning home, Mr. Sanders observed that business registration-related documents, including LLC and business filings, were missing from his home. He found a U.S. Postal Service receipt for a package mailed by U.S. Mail from his home, fraudulently using his name, and credit card information without permission, to an address in Cyprus.

70. On information and belief, Mr. Janssen took documents from Mr. Sanders' home and mailed them to Cyprus, forging Mr. Sanders' name and using his personal credit card. Defendants' actions are in accordance with their pattern of exceeding their authorization in order to conduct their scheme.



**After Gaining Access to Mr. Sanders Email and Personal Information,  
Defendants Executed an Account Takeover to Steal the CipherBlade.com  
Domain from Mr. Sanders and CipherBlade PA's Control**

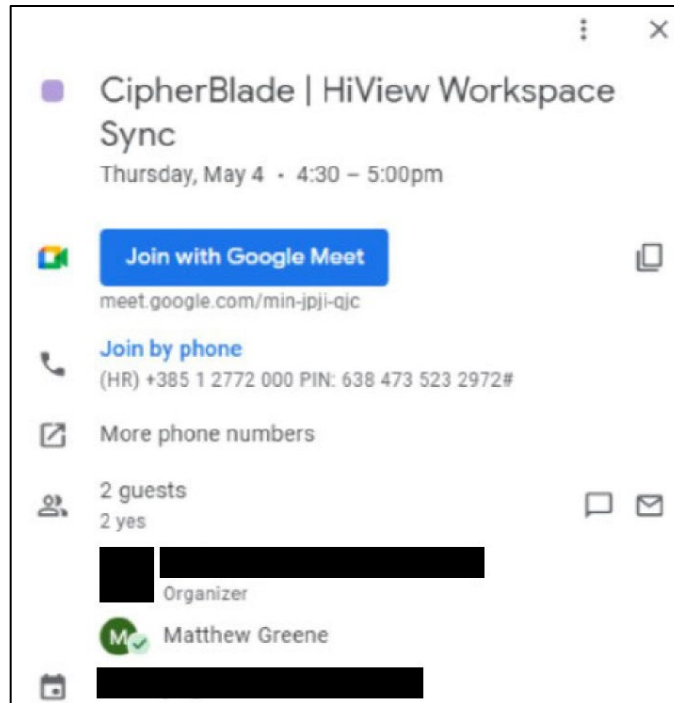
71. CipherBlade PA uses Google Workspaces to issue and manage all email addresses associated with the cipherblade.com domain. Email accounts can be established with different administrator rights depending on the privilege level associated with the account in Google Workspaces.

72. A regular user account has no administrative privileges to manage email addresses in Google Workspaces. An Administrator level account *does* have administrative rights. A Super Administrator level account is able to manage the functionality of the entire Google Workspaces platform, as well as control and manage the functionality of all Administrator accounts. Only a Super Administrator can change the level of an Administrator account – such as lowering its level from Administrator to a regular user with no elevated privileges in Google Workspaces.

73. On information and belief, Mr. Kriz had access to Super Administrator privileges by way of a shared email address [hq@cipherblade.com](mailto:hq@cipherblade.com).

74. HiView Solutions is a Google Cloud Premier Partner providing licenses, change management, and support services to customers, including those that leverage Google Workspaces. HiView is also able to assist with elevating user accounts to the Super Administrator level. CipherBlade PA engaged HiView to help manage its Google Workspaces platform.

75. On May 4, 2023, Mr. Kriz met with HiView. Mr. Kriz regularly uses the alias “Matthew Greene,” a practice that is well-known within CipherBlade PA and in the Defendants’ daily activities. *See Figure 6.*



**Figure 6**

76. Importantly, as shown in **Figure 6** above, this meeting took place on May 4, 2023, four days after Mr. Kriz's termination from CipherBlade PA. Mr. Kriz did not have any authority to meet with any of CipherBlade PA's vendors given his termination from the company.

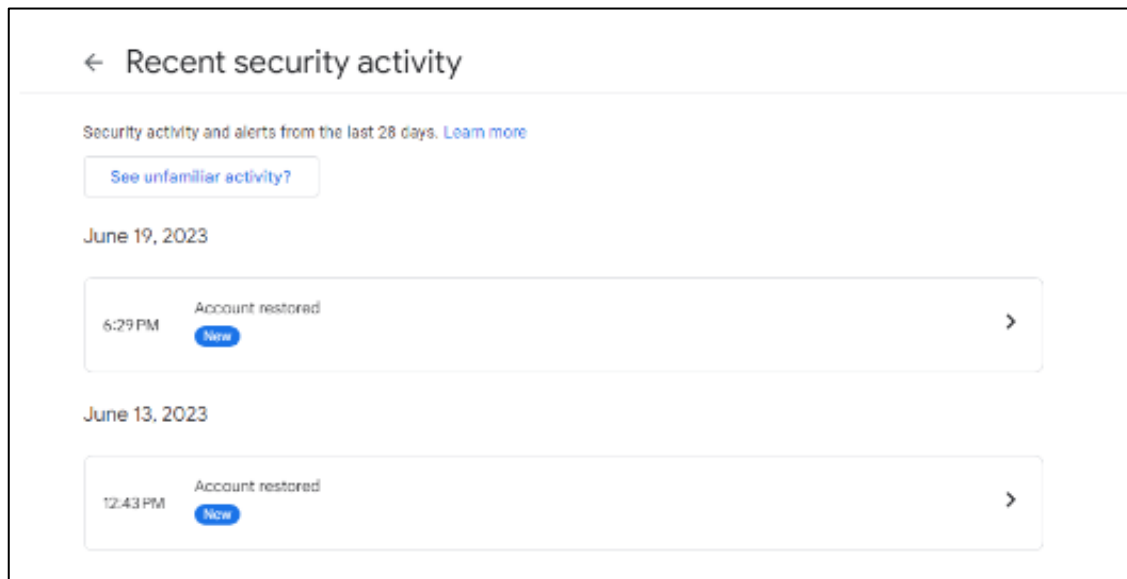
77. The cipherblade.com domain was hosted by the U.S.-based domain registrar, Namecheap, Inc. Only Mr. Sanders' email address (rich@cipherblade.com) was associated with the account on Namecheap used to manage the cipherblade.com domain. That Namecheap account had two-factor authentication (2FA) implemented, meaning that Namecheap would send an additional secret code to rich@cipherblade.com that was required to access the account. The Namecheap account solely listed the registrant and owner of the domain as CipherBlade PA.

78. Mr. Sanders did not share access to his real email address (rich@cipherblade.com) with the Defendants, so no one other than Mr. Sanders himself was able to access the contents of his email account.

79. On June 13, 2023, Defendants disabled the rich@cipherblade.com email address, thereby removing Mr. Sanders access to his company's website, related services, and any communications sent to his email address. This also prevented Mr. Sanders from receiving an email associated with the 2FA secret code from a Namecheap login attempt.

80. Plaintiff's review of the email access logs associated with the rich@cipherblade.com account in fact indicate that on June 13, 2023, the Defendants disabled Mr. Sanders' access to the rich@cipherblade.com email address and then mysteriously restored that access later that same day.

81. On information and belief, Defendants disabled Mr. Sanders' access, executed an account takeover with Namecheap as noted below, then re-enabled Mr. Sanders' account after completing the account takeover. *See Figure 7* below.



**Figure 7**

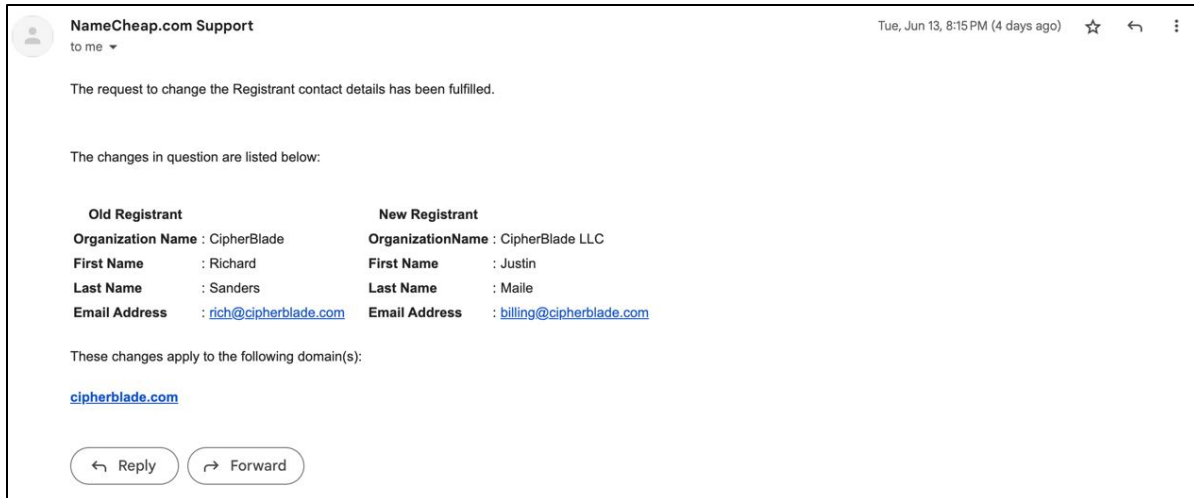
82. Also, on June 13, 2023, the Defendants changed the contact and account ownership information of the Namecheap account that was associated with cipherblade.com from rich@cipherblade.com to billing@cipherblade.com.

83. Only the Defendants have control and manage the billing@cipherblade.com email address. This means that the 2FA secret code would now be sent to Defendants and not to Mr. Sanders. This change allowed Defendants to steal the Namecheap account and cipherblade.com from Mr. Sanders.

84. On information and belief, Defendants could only have accessed the Namecheap account to make these changes by abusing the Super Administrator privileges to access Mr. Sanders' email messages without his authorization. The reason Defendants did this is because Namecheap would send the 2FA secret code only to Mr. Sanders' email address.

85. On information and belief, Defendants used that same Super Administrator access to (i) disable Mr. Sanders' access to email inbox when his account received the 2FA secret code, and (ii) create a mail forwarding rule to allow Defendants to intercept email from Mr. Sanders' email address (rich@cipherblade.com) so that they could acquire the 2FA secret code.

86. Because the Defendants have changed the account Namecheap account ownership details to reflect that billing@cipherblade.com is now the account owner – an email address that only the Defendants control – the Defendants have stolen control of the Namecheap account, usurped control of all domain management functionality from CipherBlade PA, and wrongfully converted the domain and its control to the fraudulent CipherBlade Entities operated by Defendants. *See Figure 8.*



**Figure 8**

87. Since this fraudulent account takeover, Plaintiff and Mr. Sanders have not been able to regain control over the cipherblade.com domain.

88. Mr. Sanders' authentic email address ([rich@cipherblade.com](mailto:rich@cipherblade.com)) was a Super Administrator account on Google Workspaces. However, at some point in time, Mr. Sanders opted to demote this address to Administrator, leaving the [hq@cipherblade.com](mailto:hq@cipherblade.com) address, to which he still had access, as the sole Super Administrator.

89. On or before June 16, 2023, Defendants demoted Mr. Sanders' email address ([rich@cipherblade.com](mailto:rich@cipherblade.com)) from an Administrator level account to a normal user account, thereby removing Mr. Sanders' privileges to manage any account associated with the CipherBlade PA infrastructure, including and especially the Defendants' accounts. Additionally, on or before June 16, 2023, the Defendants changed the login credentials for the [hq@cipherblade.com](mailto:hq@cipherblade.com) Super Administrator account so that Mr. Sanders had no administrative privileges whatsoever, and no ability to assess or control the Defendants' subsequent actions.

90. On July 3, 2023, Plaintiff's counsel provided Defendants' counsel with a courtesy copy of the Complaint filed on June 30, 2023. The relief requested in the Complaint included the return of the cipherblade.com domain.

91. That same day, July 3, 2023, Defendants utilized their illicit access to the stolen Namecheap account and transferred the domain from Namecheap, a U.S.-based registrar, to OVH SAS, a domain name registrar located in France. Whois data from the Domain Name System shows the exact date and time that Defendants updated and transferred the domain. *See Figure 9.*

```
Domain Name: cipherblade.com
Registry Domain ID: 2284689169_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ovh.com
Registrar URL: https://www.ovh.com
Updated Date: 2023-07-03T17:12:16Z
Creation Date: 2018-07-12T15:26:22Z
Registrar Registration Expiration Date: 2025-07-12T15:26:22Z
Registrar: OVH, SAS
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: omega3zone Global Ltd
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CY
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: REDACTED FOR PRIVACY - Send message to contact by visiting https://www.ovhcloud.com,
```

**Figure 9**

92. Also, on July 3, 2023, the Defendants altered the ownership information of the domain. The Defendants changed the owner of the domain to “omega3zone Global Ltd.” and changed the registrant country to Cyprus. *See Figure 10.*

```

Domain Name: cipherblade.com
Registry Domain ID: 2284689169_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ovh.com
Registrar URL: https://www.ovh.com
Updated Date: 2023-07-03T17:12:16Z
Creation Date: 2018-07-12T15:26:22Z
Registrar Registration Expiration Date: 2025-07-12T15:26:22Z
Registrar: OVH, SAS
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: omega3zone Global Ltd
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CY
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: REDACTED FOR PRIVACY - Send message to contact by visiting https://www.ovhcloud.com,

```

Figure 10

93. Omega3zone is a Cyprus-based company that was filed on November 15, 2022, and is owned by Defendants Mr. Marnitz and Ms. Vidrasan, who was hired to be Mr. Sanders' assistants. *See* Figure 11.

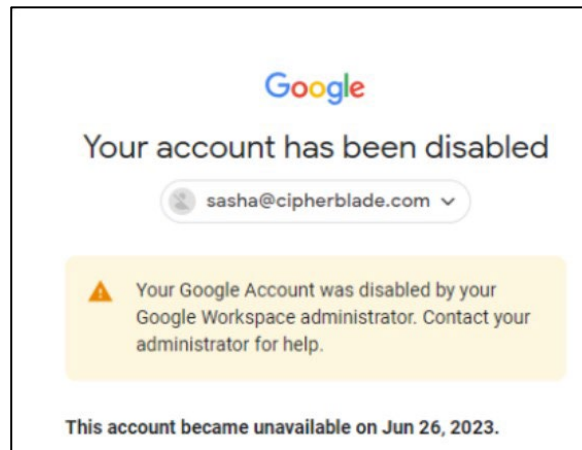
OMEGA3ZONE GLOBAL LTD	
Company Number	HE440393
Status	Active
Incorporation Date	15 November 2022 (8 months ago)
Company Type	Limited Company
Jurisdiction	Cyprus
Registered Address	Ελλάδος, 9, STELMIO BUILDING, Floor 3, Flat/Office 301 8020, Πάφος, Κύπρος Cyprus
Directors / Officers	IOANA-MARIA VIDRASAN, director IOANA-MARIA VIDRASAN, secretary PAUL BENEDICT QUINTUS MARNITZ, director
Registry Page	<a href="https://efiling.drcor.mcit.gov.cy/Drc...">https://efiling.drcor.mcit.gov.cy/Drc...</a>

Figure 11

**After Gaining Access to the CipherBlade PA Domain Name,  
Defendants Took Control of CipherBlade's IT Infrastructure to Further Their Scheme**

94. After gaining access to CipherBlade PA's Domain and the related functions, Defendants were able to take control of various CipherBlade PA-controlled IT infrastructure,

through various unauthorized administrative changes, and Defendants' continued abuse of administrative permissions. Furthermore, Defendants locked out and/or heavily restricted access to critical company infrastructure for other contractors who had raised questions and sought justification from Defendants for their activities. *See* **Figure 12**.



**Figure 12**

95. In addition to taking control of the CipherBlade PA domain name (cipherblade.com), Defendants also took control of the domain name's web hosting account with Google, the customer relationship management (CRM) tools to respond to inbound inquiries, as well as the backend IT infrastructure that is hosted with Google Workspaces, which grants contractors email access.

96. After gaining access to the infrastructure, the Defendants revoked access to CipherBlade PA IT infrastructure for Mr. Sanders as well as CipherBlade PA contractors not part of Defendants' conspiracy.

97. Because Defendants have taken control of the CipherBlade domain name, its hosting, and the back-end IT infrastructure of the company, at this moment, CipherBlade PA has been locked out of, and no longer has access to, important business generation data, customer contact information, and communications with customers.



98. In addition, Defendants have converted Plaintiff's cloud assets including confidential and trade secret business and customer information on these computer systems, with the intent to steal clients and misappropriate client funds.

**After Defendants Gained Access to CipherBlade PA's Internal Systems,  
They Continually Make Misrepresentations to Customers in an Effort to  
Move CipherBlade PA's Existing and Prospective Customer's to Their Fraudulent Entities**

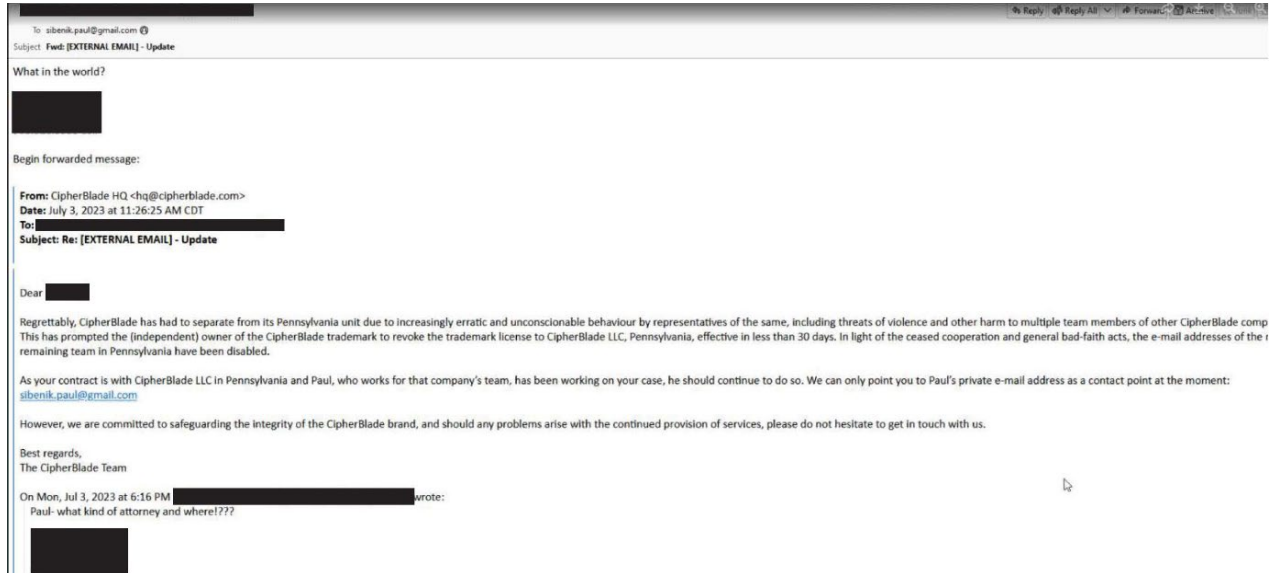
99. Defendants confused customers by making misrepresentations about CipherBlade's location in Pennsylvania, changing the cost of services, and wrongfully converting CipherBlade PA customers from the Alaska Entity.

100. Defendants have used the converted domain and website to make false statements of material fact in advertising about their services. This includes passing off the experience, expertise and tools of Plaintiff as their own. The cipherblade.com website that they converted and now control falsely, lists Mr. Sanders' personal professional certification, as evidence of their Chainalysis certification. Further, the website lists various law firms as references that are in fact the references of Plaintiff CipherBlade PA (Mr. Sanders and Mr. Sibenik). The website further contains sections entitled "Our Network" and "In the Press," referencing articles concerning Plaintiff and Plaintiff's work prior to Defendants' takeover of the website and domain, including Mr. Sanders' and Mr. Sibenik's media and press appearances.

101. The CipherBlade website includes a blog with posts written primarily by Mr. Sibenik for Plaintiff but Defendants have removed his name as author and now misleadingly list 'CipherBlade' as an author. The website also falsely makes claims about Defendants' experience that are in fact the experience of Plaintiff. Indeed, it falsely claims that Defendants have recovered millions of dollars of stolen cryptocurrency and have investigated and tracked Bitcoin belonging to suspects in hundreds of cybercrime cases. This is the experience of Plaintiff. Finally, the website makes the false claim that "We have served as expert witnesses on major

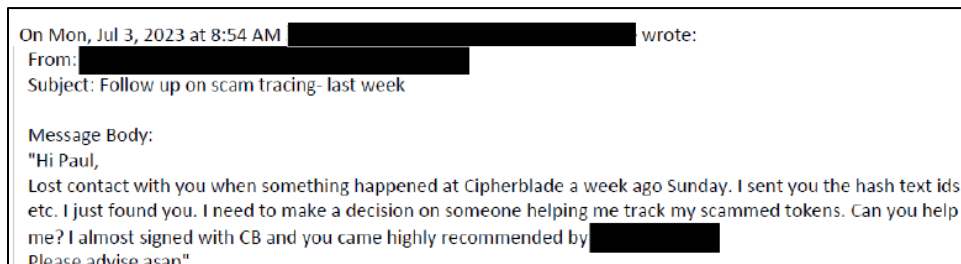
cases.” This, once again, is Plaintiff’s experience and not that of Defendants. On information and belief, Defendants have not been a witness in any litigation.

102. Defendants engaged in active outreach to clients, as depicted in the email below in **Figure 13**, circulating misrepresentations to its clients in an effort to malign the reputation of CipherBlade PA and its founder, Mr. Sanders.



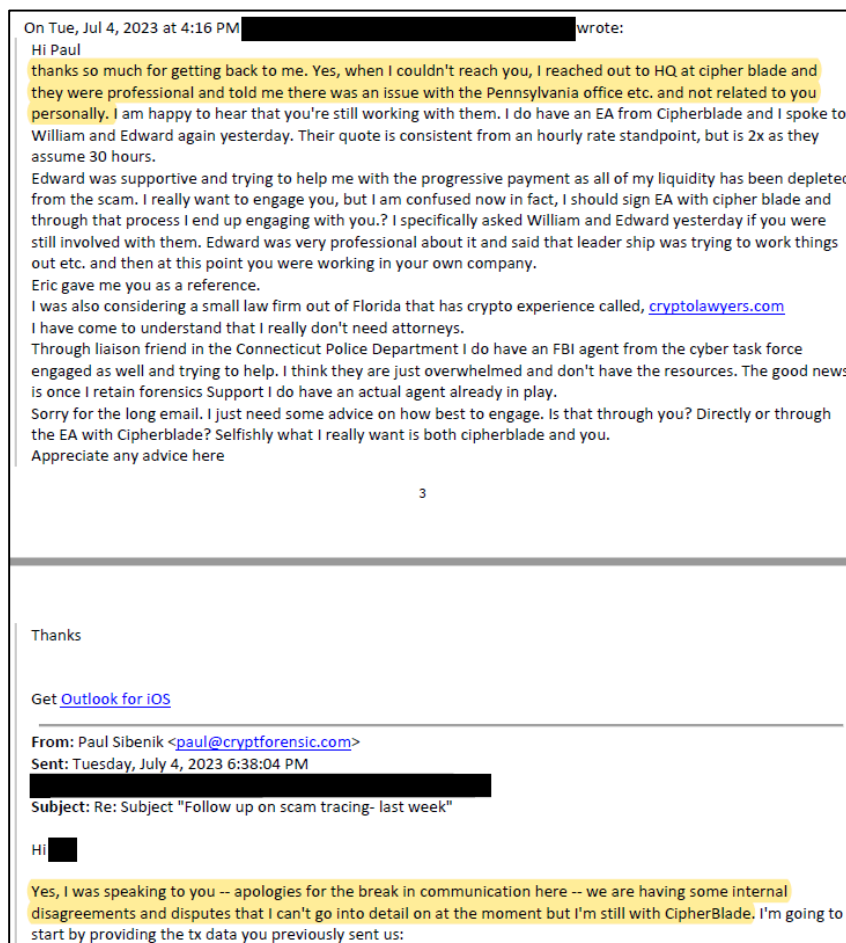
**Figure 13**

103. On July 3, 2023, a prospective CipherBlade PA customer emailed Mr. Sibenik directly to ask about his services and explains, “Lost contact with you when something happened at CipherBlade a week ago Sunday.” See **Figure 14**.



**Figure 14.**

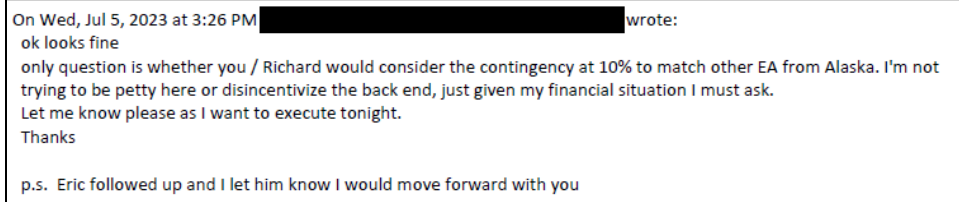
104. On information and belief, Defendants made misrepresentations to the customer, about working with CipherBlade PA. On July 4, 2023, a client emailed Mr. Sibenik explaining that, "Yes, when I couldn't reach you, I reached out to HQ at cipher blade [sic] and they were professional and told me there was an issue with the Pennsylvania office etc. And not related to you personally." It appears that the client believes "HQ" to be different from their "Pennsylvania office." See **Figure 15**.



**Figure 15**

105. Defendants also confused the customer by providing services at a different price than CipherBlade PA would charge. In negotiations with Mr. Sibenik, the client writes, "on

question is whether you / Richard would consider the contingency at 10% to match other EA from Alaska . . . Eric followed up and I let him know I would move forward with you.” See **Figure 16**.

A screenshot of a text message conversation. The text is as follows:

On Wed, Jul 5, 2023 at 3:26 PM [REDACTED] wrote:  
ok looks fine  
only question is whether you / Richard would consider the contingency at 10% to match other EA from Alaska. I'm not trying to be petty here or disincentivize the back end, just given my financial situation I must ask.  
Let me know please as I want to execute tonight.  
Thanks  
p.s. Eric followed up and I let him know I would move forward with you

**Figure 16**

106. Defendants also began accepting payments which clients believed was being sent to CipherBlade PA.

107. In July 2023, one CipherBlade PA client sent Defendants a communication on Telegram, a secure messaging app CipherBlade PA uses, explaining, “I don’t understand how we paid the wrong CipherBlade group when I specifically asked for Paul and they said you don’t work for them anymore. This is very frustrating because I don’t know who to believe and y’all are from the same company.” This CipherBlade PA client, as a result of Defendants’ misrepresentations, mistakenly paid the Alaska Entity \$30,000 USD instead of CipherBlade PA, with whom they assumed they were engaging. See **Figure 17**.

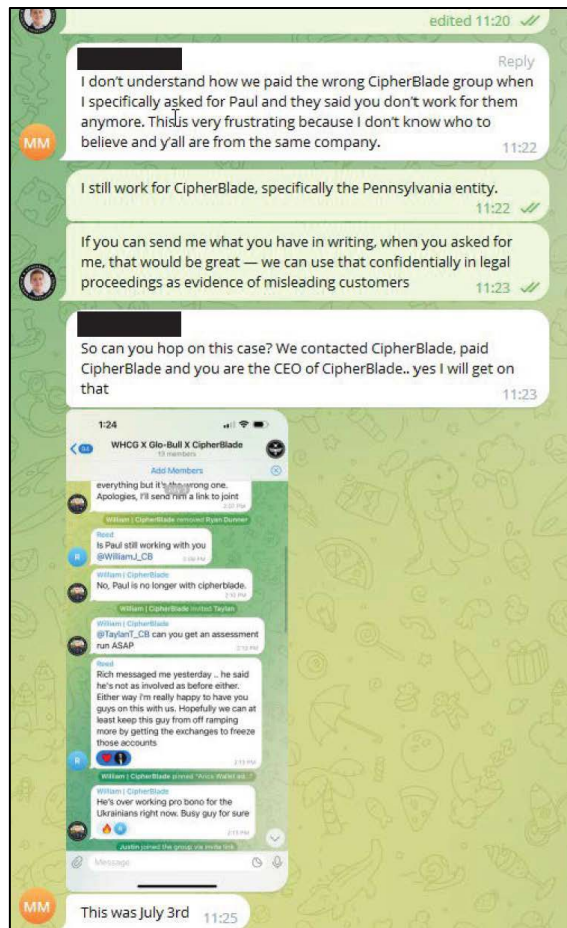


Figure 17

108. This CipherBlade PA client then wrote to Mr. Sibenik explaining, “we just paid them 30k and they are refusing a refund how do I justify paying the same company another 20k for another team to do the first teams job.” The CipherBlade PA client continued, evidencing the harm now being caused Plaintiff, “we went to the FBI and they told us this was the best route.” See **Figure 18**, below.

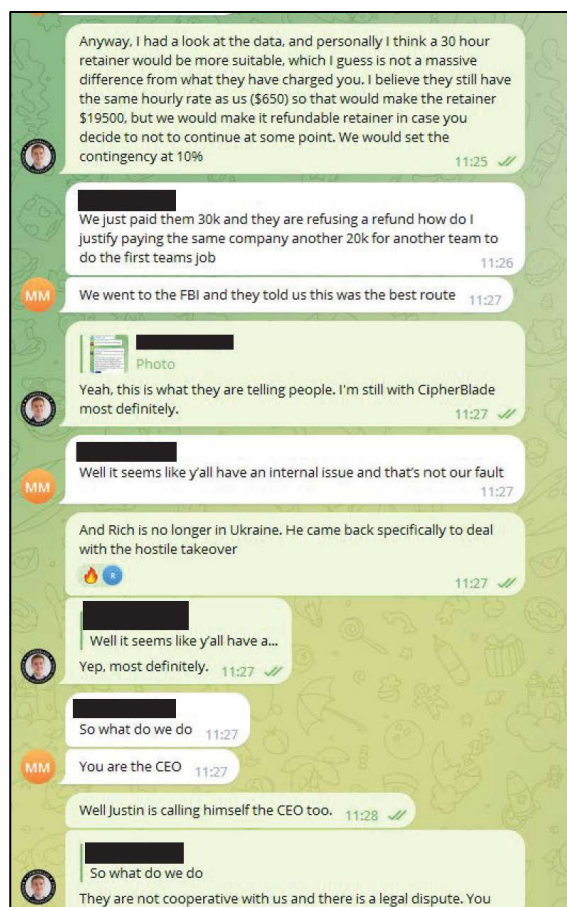
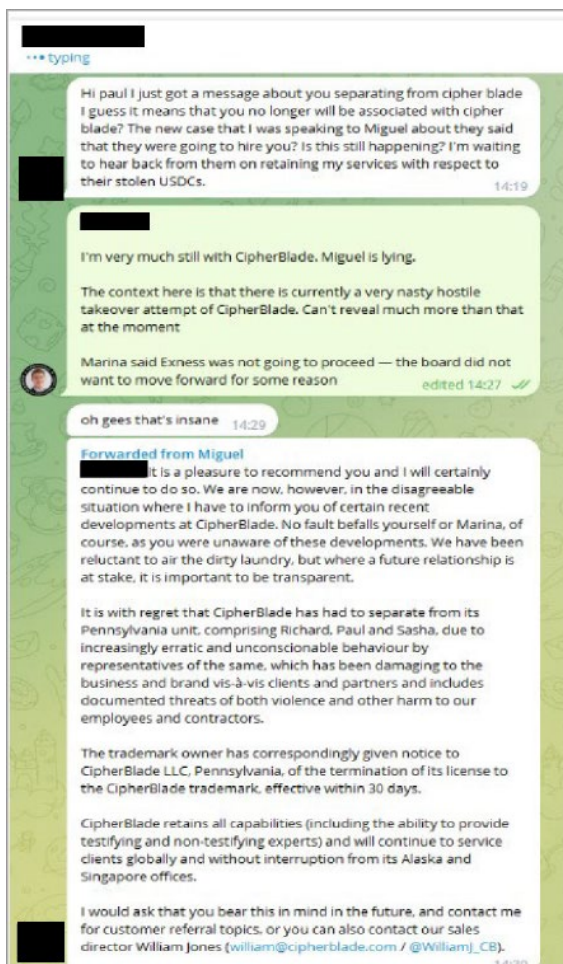


Figure 18

109. The Defendants also engaged in slanderous misrepresentation in an effort to capture existing CipherBlade PA clients. For example, in June 2023, an active client messaged Mr. Sibenik questioning if he was separating from CipherBlade PA. The client forwarded a message from Defendant Sergio Garcia (who used the alias Miguel Alonso Torres) in which he represents that “CipherBlade has had to separate from its Pennsylvania unit, comprising Richard, Paul, and Sasha....” This message makes additional disparaging remarks about Mr. Sibenik, Mr. Sanders and another CipherBlade PA employee not involved in the scheme, Nevena Lazić (otherwise referred to as “Sasha”) and requests that the client contact his CipherBlade email in the future. This is a prime example of how Defendants worked to interfere with CipherBlade’s existing relationships

and have caused irreparable harm to the Plaintiff. *See Figure 19*, which takes place on June 22, 2023, on Telegram.



**Figure 19**

110. Defendants' misrepresentation and fraudulent activities have directly resulted in the loss of client engagements.

111. On June 5, 2023, CipherBlade PA entered into an Engagement Agreement with a potential client a citizen of the United Kingdom. The client engaged CipherBlade PA to perform investigative and expert services in the domain of blockchain forensics and cryptocurrencies.

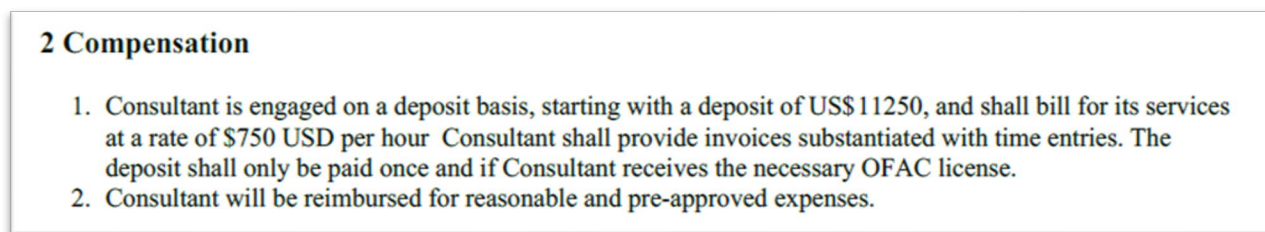


Below is an accurate representation of the Engagement Agreement between CipherBlade PA and the client. *See Figure 20.*



**Figure 20**

112. The contract included a deposit of \$11,250 USD. An accurate copy of the compensation provisions is shown below. *See Figure 21.*



**Figure 21**

113. The client attempted to conduct additional business with CipherBlade PA and attempted to reach Mr. Sibenik at his paul@cipherblade.com email address, however, due to Defendants' fraudulent takeover and subsequent restriction of CipherBlade PA's employee's privileges, Mr. Sibenik no longer had access to his work email.

114. Defendants' subsequent misrepresentations and false narratives to the client subsequently led to the client's withdrawal of their engagement with CipherBlade PA on July 12, 2023. Below is an accurate representation of the email from the client to Mr. Sibenik terminating the engagement. *See Figure 22.*



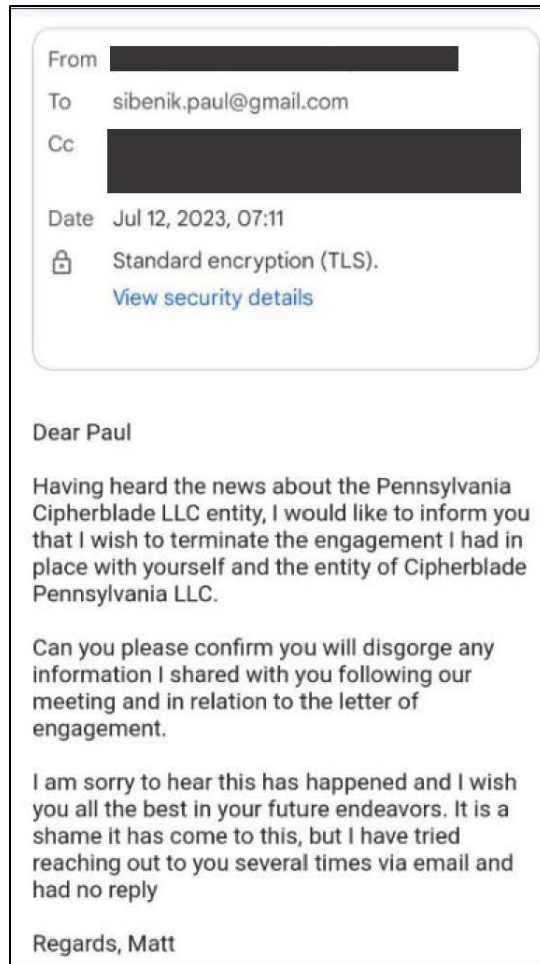


Figure 22

**Defendant Siphoned Off Funds from CipherBlade PA  
 Using the Fraudulent CipherBlade Entities and Shell Companies**

115. Not only were the Defendants actively working to steal trade secrets, proprietary information and clients from CipherBlade PA, the Defendants were actively stealing and misappropriating funds from CipherBlade PA.

116. Mr. Sanders entrusted Mr. Kriz and Mr. Krause with handling routine transactions on behalf of CipherBlade PA. This means that Mr. Kriz and Mr. Krause had access to the CipherBlade PA Wise financial accounts, which they used for regular payments, and unfortunately, to siphon and misappropriate funds.

117. CipherBlade PA's business accounts are in Wise, a money services provider that focuses on holding and converting currencies. CipherBlade PA has accounts in five different currencies, including U.S. dollars (USD), Euro (EUR), the British Pound (GBP), Australian dollar (AUR), and Canadian dollar (CAD). For every currency, CipherBlade LLC in Pittsburgh, PA is listed as the account holder. Here, relevant transactions were made from USD, EUR, and GBP accounts. See **Figure 23**.

<b>EUR statement</b>	<b>GBP statement</b>	<b>USD statement</b>
January 1, 2023 [GMT-04:00]	January 1, 2023 [GMT-04:00]	January 1, 2023 [GMT-04:00]
Generated on: June 20, 2023	Generated on: June 20, 2023	Generated on: June 20, 2023
<b>Account Holder</b> CipherBlade LLC 7070 FORWARD AVE APT 402 Pittsburgh PA 15217 United States	<b>Account Holder</b> CipherBlade LLC 7070 FORWARD AVE APT 402 Pittsburgh PA 15217 United States	<b>Account Holder</b> CipherBlade LLC 7070 FORWARD AVE APT 402 Pittsburgh PA 15217 United States

**Figure 23**

118. Upon review of CipherBlade PA's financial records it was discovered that in 2023, after Mr. Sanders departed for Ukraine, \$24,700 USD was transferred to the Singapore Entity.

119. CipherBlade PA does not pay for consulting or advisory services. However, upon review of CipherBlade PA's financial records, several transactions to unknown companies that appear to be consulting or advisory service companies, were discovered.

120. CipherBlade PA discovered that in 2022, \$417,577.31 (USD) and € 48,767.88 (EUR) was transferred from CipherBlade PA to Green Stone Advisory FZ-LLC ("Green Stone"). In 2023, \$720,238.13 (USD) was transferred to the same entity. Mr. Sanders did not authorize these payments.

121. CipherBlade PA investigated these charges and established it never entered into a contract with Green Stone.

122. Upon information and belief, Green Stone is a shell company connected to the Defendants and was used to wrongfully transfer funds out of CipherBlade PA.

123. CipherBlade PA discovered that in 2022, \$150,000 was transferred from CipherBlade PA to White Orchard Ltd. White Orchard is owned by Defendant Manuel Kriz. See **Figure 24.**

<b>WHITE ORCHARD CAPITAL LTD</b>	
Company Number	HE423785
Status	Active
Incorporation Date	19 July 2021 (almost 2 years ago)
Company Type	Limited Company
Jurisdiction	<a href="#">Cyprus</a>
Registered Address	<ul style="list-style-type: none"> <li>• Ελλάδος, 9, STELMIO CENTER, Floor 1, Flat/Office 102</li> <li>• 8020, Πάφος, Κύπρος</li> <li>• Cyprus</li> </ul>
<a href="#">Directors / Officers</a>	<ul style="list-style-type: none"> <li>• <a href="#">MANUEL KRIZ</a>, director</li> <li>• <a href="#">MANUEL KRIZ</a>, secretary</li> </ul>

**Figure 24**

124. CipherBlade PA investigated these charges and established it never entered into a contract with White Orchard Ltd.

125. Upon information and belief, White Orchard Ltd., is a shell company connected to the Defendants and was used to wrongfully transfer funds out of CipherBlade PA.

126. CipherBlade PA discovered that in April 2023, \$110,636.42 (USD) and €345,675.91 (EUR) was transferred from CipherBlade PA to Inquisita Solutions, a Cyprus-based company.

127. CipherBlade PA investigated these charges and established it never entered into a contract with Inquisita Solutions.

128. Upon information and belief, Inquisita Solutions is a shell company owned by Mr. Kriz and Mr. Janssen.

129. Overall, \$1,451,589.64 (USD) and €294,443.79 (approximately \$330,655.96 USD) was wrongfully transferred to Green Stone, White Orchard Ltd., the Singapore Entity, and CipherBlade Ltd.,

130. All of these amounts have been converted from CipherBlade PA to the fake CipherBlade operations and various shell companies.

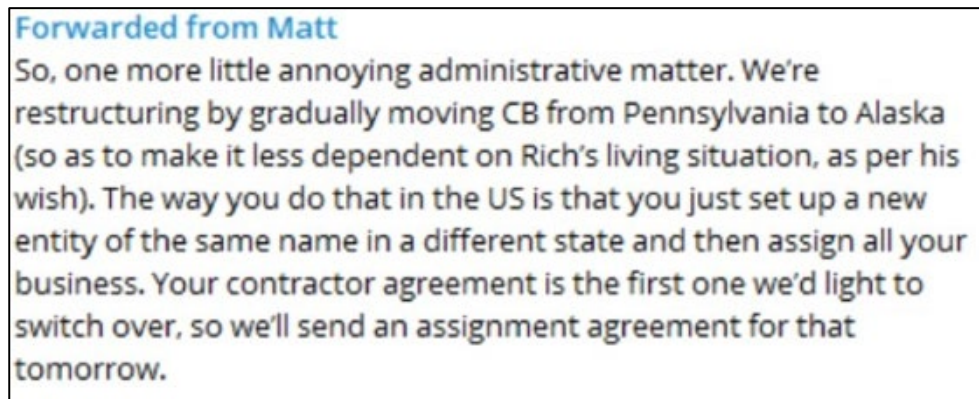
**Defendants Engaged in Significant Criminal Activity and Operated a Racketeering Style Enterprise Scheme to Siphon Off Funds, Trade Secrets and Clients from CipherBlade PA**

131. Furthermore, on June 16, 2023, Mr. Sibenik, the CEO of CipherBlade PA, became aware that there was a ‘hostile takeover’ of CipherBlade PA. He found that Defendants had discreetly been orchestrating considerable changes in the weeks and months prior. In this time period, for example, they perpetuated the false narrative that Mr. Sanders approved of business contracts being transferred from CipherBlade PA to the Alaska Entity, when in fact that was accomplished by falsely representing to Mr. Sanders that the Alaska Entity would be set up as owned by Mr. Sanders.

132. Defendants also actively attempted to solicit payments from numerous current CipherBlade PA clientele over to the Alaska Entity.

133. Because the CipherBlade PA employees who are not part of Defendants' conspiracy do not have visibility into client emails (because Defendants have locked them out of email access), it is currently impossible to know the full extent of the harm done.

134. For example, Mr. Kriz encouraged multiple CipherBlade PA contractors to send invoices for large bonuses to be paid by CipherBlade PA, in an attempt to curry favor with them, days before their contractor agreements were fraudulently assigned to the Alaska Entity. *See Figures 25 and 26.*



**Forwarded from Matt**  
So, one more little annoying administrative matter. We're restructuring by gradually moving CB from Pennsylvania to Alaska (so as to make it less dependent on Rich's living situation, as per his wish). The way you do that in the US is that you just set up a new entity of the same name in a different state and then assign all your business. Your contractor agreement is the first one we'd light to switch over, so we'll send an assignment agreement for that tomorrow.

**Figure 25**

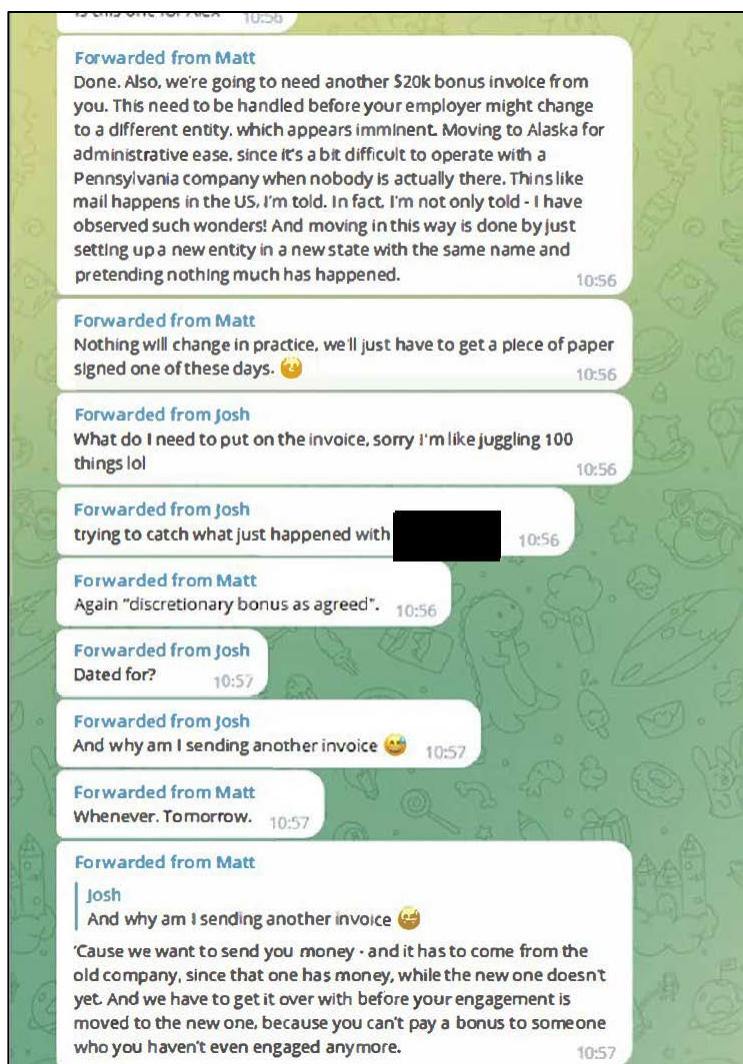


Figure 26.

135. Defendants then used this inappropriate scheme and fraudulent partnerships to tout aggressive growth and try to solicit new clients that should have engaged CipherBlade PA as well as some current CipherBlade PA clients. *See Figure 27*, related to a conversation with Mr. Maile on May 1, 2023, through a “CipherBlade Operations Main” group chat in the messaging platform, Telegram, initially created to use for CipherBlade PA business.



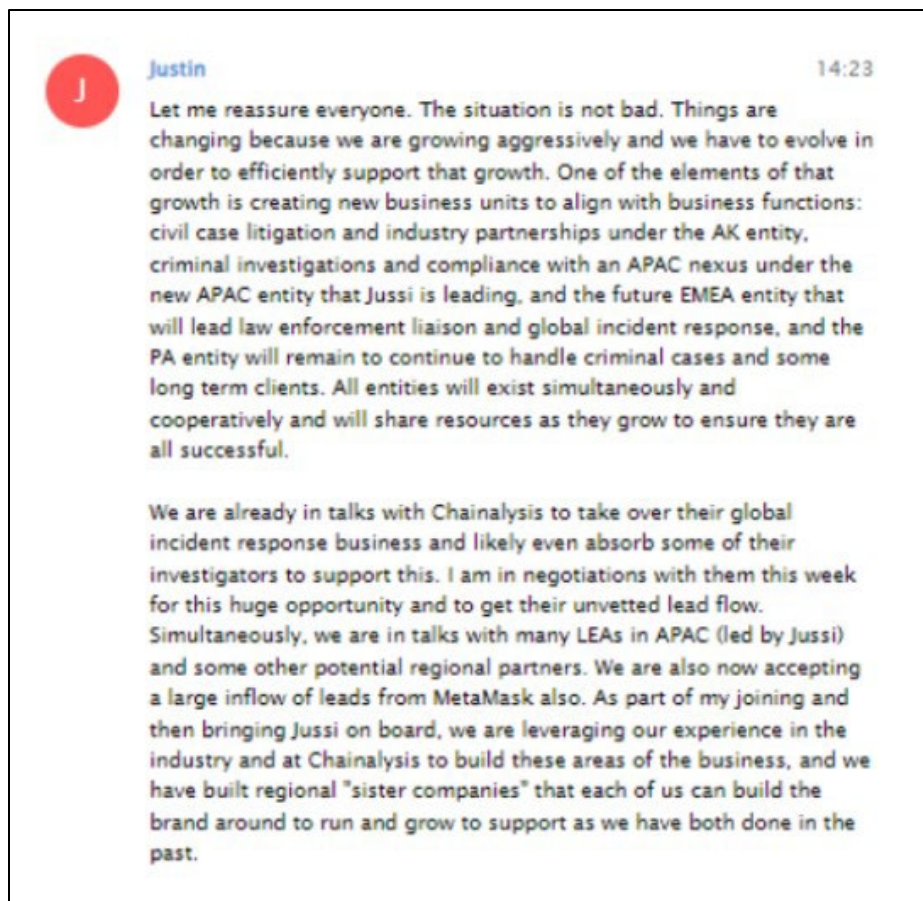


Figure 27

136. Defendants also converted CipherBlade PA's corporate assets by making payments with to themselves, making the payment as vendor payments to entities controlled by Defendants.

137. For example, Defendants transferred CipherBlade PA funds in a series of transactions captured as "Management Services" and "Consulting." These payments were made from CipherBlade PA's Wise business account to a shell company called Inquisita Solutions Ltd. in multiple instances across the month of April 2023 and just days before Mr. Kriz was fired from CipherBlade PA. According to Inquisita Solutions Ltd.'s records, the entity's Director and Secretary are listed as Mr. Kriz and Mr. Janssen. Defendants also have asserted control, without authority, over some of CipherBlade PA's cryptocurrency assets. *See Figure 28.*

INQUISITA SOLUTIONS LTD	
Company Number	HE443355
Status	Active
Incorporation Date	3 February 2023 (5 months ago)
Company Type	Limited Company
Jurisdiction	<a href="#">Cyprus</a>
Registered Address	<ul style="list-style-type: none"> <li>• Ελλάδα, 9, STELMIO BUILDING, Floor 1, Flat/Office 102</li> <li>8280, Πάφος, Κύπρος</li> <li>• Cyprus</li> </ul>
<a href="#">Directors / Officers</a>	<ul style="list-style-type: none"> <li>• <a href="#">JORN HENRIK BERNHARD JANSSEN</a>, secretary</li> <li>• <a href="#">MANUEL KRIZ</a>, director</li> </ul>

**Figure 28**

138. Defendants actively engaged in a series of unauthorized and unlawful activities that sought to undermine the control and ownership of CipherBlade PA. Defendants also perpetuated their efforts by abusing the access Mr. Sanders granted them to his home while he was away in Ukraine, including the theft of CipherBlade PA corporate documents from his home.

139. While abroad in Ukraine, Mr. Sanders received a series of alerts from his home security system of that indicated all of his security cameras suddenly went offline. Upon his return home, he observed that business registration related documents, including LLC and business filings, were missing.

140. Furthermore, he came across a U.S. Postal Service receipt for a package purportedly mailed by U.S. Mail from his home, fraudulently using his name, and credit card information without permission, sent to an address in Cyprus. On further inspection of the receipt, the package was addressed to Mr. Marnitz, Mr. Krause's son, in Cyprus.



141. Mr. Krause is no stranger to the above-mentioned types of financial theft, criminal enterprise, and associated violence, evidenced by his six-year prison sentence for the theft of 3.7 million Euros from the German textile discounter, NKD. Furthermore, Mr. Krause was subsequently sentenced for his attempt to persuade two members of the Russian Mafia in the Czech Republic to kidnap and murder Judge Bösemesser, who was presiding over his case. *See* <https://www.kurier.de/inhalt.warum-michael-krause-im-urteil-des-schwurgericht-hof-fuer-sein-knast-komplott-dennoch-vergleichsweise-gut-davon-kommt-hof-ex-nkd-chef-kriegt-fuenf-jahre-mehr.8f9c8714-9eb9-40a7-be64-35714096a972.html>.

## **CAUSES OF ACTION**

### **COUNT I**

#### **MISAPPROPRIATION OF TRADE SECRETS**

#### **DEFEND TRADE SECRETS ACT, 18 U.S.C. § 1836**

142. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

143. Plaintiff is the owner of the Trade Secrets and Confidential Information, which includes proprietary investigative techniques and processes, confidential business information and trade secrets concerning the ongoing relationship with Chainalysis, and information concerning specific clients and matters as well as new prospective clients and matters. The Trade Secrets and Confidential Information are intended for use in interstate and/or foreign commerce, including in the execution of business contracts for conducting blockchain investigations and tracking of Bitcoin and other cryptocurrencies in cybercrime cases.

144. Plaintiff's Trade Secrets and Confidential Information derive independent economic value from not being known to the public or other persons who could obtain

economic value from their disclosure or use.

145. Plaintiff takes reasonable measures under the circumstances to keep their Trade Secrets and Confidential Information confidential.

146. Defendants misappropriated Plaintiff's Trade Secrets and Confidential Information by wrongfully obtaining them through fraudulent and other unlawful acts and/or using Plaintiff's Trade Secrets and Confidential Information wrongfully obtained.

147. Plaintiff identified repeated instances of misappropriation by Defendants, including those described above.

148. Defendants know or should know that Plaintiff's Trade Secrets and Confidential Information were acquired by improper means.

149. Defendants have improperly disclosed and/or used Plaintiff's Trade Secrets and Confidential Information after improperly acquiring them, including to compete with CipherBlade.

150. Defendants have caused and continue to cause Plaintiff damages and irreparable injury.

151. Plaintiff is entitled to a monetary award under 18 U.S.C. § 1836, including damages to Plaintiff and any diminution in the value of its Trade Secrets and Confidential Information, and the unjust enrichment of Defendants arising from Defendants' misappropriation.

152. Defendants' misappropriation is reckless, willful, and malicious and thereby entitles Plaintiff to an award of exemplary damages, as well as attorneys' fees.

153. Defendants' misappropriation of Plaintiff's Trade Secrets and Confidential Information has caused and will continue to cause Plaintiff irreparable and substantial injury

and therefore cannot be fully redressed through damages alone. An injunction prohibiting Defendants from misappropriating, using, or disclosing Plaintiff's Trade Secrets and Confidential Information in any manner, and ordering that Defendants permanently destroy any of Plaintiff's Trade Secrets and Confidential Information in their possession, custody, or control, including any materials that were in any way derived from Plaintiff's Trade Secrets and Confidential Information, is necessary to provide Plaintiff with complete relief.

## **COUNT II**

### **COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030 *et seq.***

154. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

155. Defendants wrongfully and intentionally, without authority, accessed protected CipherBlade accounts in order to take control over essential to CipherBlade assets, such as its domain name, and to gain full administrator rights over CipherBlade's IT infrastructure, on which accounts on which CipherBlade's Trade Secrets and Confidential Information resides, and from which Defendants absconded with information, account credentials, and funds, all without authorization.

156. These actions were unauthorized because Defendants never had authority to transfer assets or take over full administrative rights on these accounts, especially to the point of excluding the CipherBlade founder, Mr. Sanders, from access to his accounts.

157. As a direct and proximate result of Defendants' conduct in violation of the CFAA, CipherBlade has suffered and will continue to suffer damages in excess of \$5,000.

158. As a direct result of Defendants' actions, Plaintiff suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless

Defendants' actions are enjoined.

**COUNT III**

**UNFAIR COMPETITION, 15 U.S.C. § 1125(a)**

159. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

160. Defendants have taken over CipherBlade, and made false and misleading statements to promote their services, on information and belief, that pass off the experience, expertise and tools of Plaintiff as their own and that falsely disparage Plaintiff and its services as part of Defendants' scheme to steal customers, customer leads and to promote their services in the marketplace by false statements to the detriment of Plaintiff. Defendants have made these statements in connection with their services provided in interstate commerce.

161. Defendants' statements are false and misleading because they are passing themselves off as having Plaintiff's expertise and experience in its investigative and/or expert witness services among Plaintiff's customers, partners and in the marketplace.

162. Defendants made these false and misleading statements on their website, to Plaintiff's customers and in the marketplace knowing they were false and misleading and made in bad faith to mislead Plaintiff's customers, partners and the marketplace for such investigative and expert witness services.

163. Defendants' statements are likely to confuse or deceive a substantial segment of its audience in the marketplace for such investigative and expert witness services, and this deception is material, in that it is likely to influence customers' decisions about whether to engage Defendants or Plaintiff.

164. Defendants' false and misleading statements constitute unfair competition under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a).

165. Defendants' false and misleading statements tend to harm, have harmed, and will continue to harm Plaintiff and their business relationships, the conduct of their business, and their ability to obtain and maintain sales and business relationships.

166. Plaintiff has been and is likely to be injured as a result of the false and misleading statements, either by direct diversion of sales or by a lessening of the goodwill associated with its products. Plaintiff is and have been irreparably damaged in its business or property by Defendants' false and misleading statements, and unless Defendants' false and misleading statements are enjoined by this Court, Plaintiff will continue to suffer monetary damage, market price erosion, loss of market share, lost sales, and irreparable harm to its reputation, relationships, and goodwill with its customers, partners, vendors, distributors, industry professionals, and others.

#### **COUNT IV**

##### **TORTIOUS INFERENCE WITH CONTRACTS**

167. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

168. Plaintiff had valid contracts with numerous customers, contractors, and vendors. Namely, the Chainalysis contract was critical to Plaintiff's business. Because Defendants were employed by Plaintiff, they knew of Plaintiff's existing contracts with Chainalysis, as well as their customers, contractors, and vendors.

169. Despite this knowledge, Defendants endeavored to convert business relationships to entities in Alaska and Singapore under false pretense of being the same existing Plaintiff. Defendants sought to confuse clients, contractors, and vendors inducing them to break contract

with Plaintiff.

170. For example, Plaintiff relies on Reactor, Chainalysis' blockchain analysis software, to conduct its investigations. Plaintiff's contract with Chainalysis is central to their entire business. Based on a conversation between Mr. Sanders and Chainalysis, Defendant Kriz sent a request to change the Plaintiff's contract on June 13, 2023. Mr. Sanders then showed Chainalysis evidence of Defendant Kriz's termination in order to keep their original contract intact.

171. On June 22, 2023, Mr. Sanders sent Chainalysis a notarized letter to keep only four users on Reactor. This includes Mr. Sibenik, Mr. Sanders, and two of their colleagues (Josh and Sasha).

172. In other situations, Defendants actions confused clients, impacting their payment and causing irreparable harm. For example, in the chats with a CipherBlade PA client, the client stated "I don't understand how we paid the wrong CipherBlade group when I specifically asked for Paul and they said you don't work for them anymore. This is very frustrating because I don't know who to believe and y'all are from the same company."

173. Defendants knowingly interfered with Plaintiff's contracts with customers, contractors, and vendors, especially Chainalysis. As a result of Defendants actions, Plaintiff has suffered actual damages as well as irreparable damage to its reputation as a business.

## **COUNT V**

### **TORTIOUS INFERENCE WITH BUSINESS ADVANTAGE**

174. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

175. Plaintiff had business relationships with several entities, most significantly, with Chainalysis, Inc. and the use of Chainalysis' blockchain analysis software, Reactor. Plaintiff also

had business relationships with individuals located in this District and internationally that engaged Plaintiff to perform investigative and expert services in the domain of blockchain forensics and cryptocurrencies.

176. Defendants maliciously interfered with Plaintiff's business relationships, including actively soliciting businesses to transition from Plaintiff to the Alaska Entity. This includes Defendants knowingly soliciting Chainalysis to transition to engage in business solely with the Alaska Entity. In addition, Defendants also interfered with business relationships through the direct outreach to clients and circulating false and negative statements about Plaintiff in order to convert Plaintiff's business to the Alaska Entity. This includes not only corporate clients but individual clients as well.

177. Defendants acted wrongfully and purposefully when they interfered with Plaintiff's business relationships in order to avail themselves of the business benefit associated with those relationships. Plaintiff's relationship with Chainalysis was of particular importance and in their attempts to falsely establish the Alaska Entity as the authentic Plaintiff, sought to transfer without authorization, access to the Reactor software to their Alaska Entity. This effort was a direct attempt to improperly insert themselves into the established contract with Chainalysis in lieu of Plaintiff. Defendants were also dishonest in holding themselves out to have the experience and expertise of Plaintiff and perpetuating an inaccurate narrative about Plaintiff to all of Plaintiff's business relationships. Moreover, Defendants' active effort to disable the CipherBlade email addresses prevented CipherBlade from being able to retrieve any email correspondence from customers.

178. Defendants' acts injured the Plaintiff's relationship with its clients and business partners. In particular, Plaintiff lost the engagement with at least one client as a result of Defendants' activities. Defendants' activities directly prevented Plaintiff from continuing with the

customer's business relationship. Plaintiff was unable to access their official CipherBlade email addresses in order to continue communications with clients. Due to the Plaintiff's non-responsiveness and subsequent misrepresentations by the Defendants, Plaintiff lost the engagement. But for Defendants' actions, Plaintiff would have been able to continue providing investigative services to the client.

179. Plaintiff's business relationship with Chainalysis is also threatened by Defendants' schem, a significant deviation from the solid partnership previously established with Chainalysis. Although Plaintiff continues to use Reactor, the turmoil caused by Defendants' outreach to Chainalysis to convert them to the Alaska Entity has injured the important relationship, calling into question the viability of CipherBlade's ability to do business effectively and efficiently.

## **COUNT VI**

### **CONVERSION**

180. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

181. Defendants knew or should have known that taking Trade Secrets and Confidential Information was prohibited and unlawful.

182. At all relevant times, Plaintiff owned the Trade Secrets and Confidential Information contained in writing and on Plaintiff's IT infrastructure.

183. Defendants have willfully taken and exercised unlawful and unauthorized dominion and control over Trade Secrets and Confidential Information, including for their personal use and/or through disclosure to third parties.

184. Defendants converted and/or will continue to convert the Trade Secrets and Confidential Information for their own use and financial gain and without authorization or



consent from Plaintiff.

185. As a direct and proximate cause of Defendants' conversion of the Trade Secrets and Confidential Information, Plaintiff has incurred and continue to incur damages and irreparable injury, including without limitation, lost value and potential profits it would have earned but for Defendants' unlawful actions.

186. Plaintiff is entitled to recover compensatory and punitive damages from Defendants in an amount to be determined at trial.

187. Defendants' conversion of the Trade Secrets and Confidential Information has caused and will continue to cause Plaintiff irreparable and substantial injury and therefore cannot be fully redressed through damages alone. An injunction prohibiting Defendants from using, disclosing, or relying on the Trade Secrets and Confidential Information in any manner, and ordering that Defendant permanently destroy any of the Trade Secrets and Confidential Information in his possession, custody, or control, including any materials that were in any way derived from the Trade Secrets and Confidential Information, is necessary to provide Plaintiff with complete relief.

## **COUNT VII**

### **TRESPASS TO CHATTEL**

188. Plaintiff repeats and reallege each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

189. Defendants have used a computer and/or computer network, without authority, with the intent to cause injury to the property of another.

190. Defendants have used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Plaintiff.

191. Defendants' actions in operating "fake CipherBlade" involved Defendants accessing and misappropriating CipherBlade's accounts and IT infrastructure, on which CipherBlade's Trade Secrets and Confidential Information resides, and from which Defendants absconded with information, account credentials, and funds.

192. Defendants' actions have caused injury to Plaintiff and have interfered with the possessory interests of Plaintiff over its software.

193. Plaintiff seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

194. As a direct result of Defendants' actions, Plaintiff has suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

## **COUNT VIII**

### **FRAUD**

195. Plaintiff repeats and reallege each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

196. Upon information and belief, Defendants' main objective was to commit a hostile takeover of Plaintiff's business and to collect money to which they are not entitled.

Defendants have taken over accounts, IT infrastructure on client relationships to which they are not entitled.

197. CipherBlade Alaska and Singapore continue using stolen corporate assets to pass themselves off as the real CipherBlade, profiting from assets stolen from CipherBlade Pennsylvania and UK entities. They continue to make false representations to business contacts, intending to steal additional assets from the real CipherBlade.

198. Defendants also committed fraud when they exceeded their limited administrative access and authority to convert trade secrets and confidential information, such as employee and business contracts, to their control. Defendants represented that Mr. Sanders approved of the actions taken. He did not. For example, on information and belief, Defendants forged Mr. Sanders' signature on contracts assigning CipherBlade contractors to the Alaska Entity. While the Defendants claim Mr. Sanders signed this document, the Internet Protocol (IP) address it was signed from geolocates to Pennsylvania during which time Mr. Sanders was located in Ukraine.

199. Defendants took control of the CipherBlade domain and changed contact information on the website from Pennsylvania to the entities in in Alaska and Singapore, wrongfully representing themselves as the appropriate points of contact. Defendants do not have and have never had authority to control the CipherBlade domain, and CipherBlade's appropriate contact is still based in Pennsylvania.

200. Defendants also used Mr. Sanders' email to contact customers and business contacts on behalf of and as Mr. Sanders himself. Defendants knowingly contacts others using Mr. Sanders' name to induce confusion from customers and business contacts, misrepresenting Mr. Sanders' actions and beliefs at that time.

## **COUNT IX**

### **UNJUST ENRICHMENT**

201. Plaintiff repeats and reallege each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

202. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Plaintiff in violation of the common law. Defendants used, without authorization or license, software, information, and infrastructure belonging to Plaintiff to

facilitate unlawful conduct inuring to the benefit of Defendants.

203. Defendants profited unjustly from their unauthorized and unlicensed use of Plaintiff's intellectual property.

204. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Plaintiff's intellectual property.

205. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

206. Plaintiff seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

207. As a direct result of Defendants' actions, Plaintiff suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **COUNT X**

#### **VIOLATION OF RICO, 18 U.S.C. § 1962() and (D)**

208. Plaintiff repeat and reallege each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

209. At all relevant times, CipherBlade LLC was a "person" within the meaning of RICO, 18 U.S.C. §§ 1961(3) and 1964(c) and (d).

210. At all relevant times, the Defendants were "persons" within the meaning of RICO, 18 U.S.C. §§ 1961(3) and 1964(c) and (d).

211. As alleged above, the RICO Defendants are each comprised of natural persons and of corporate entities that they formed to carry out the unlawful activities described above.

212. The Defendants are each comprised of natural persons and of corporate entities that are formed to carry out the unlawful activities described above. They have continuously and effectively carried out their purpose of taking over the CipherBlade IT infrastructure, including the domain name and website registrar. The Defendants have used the misappropriated infrastructure in the furtherance of the scheme to steal current clients and divert future clients to the Defendants. This association-in-fact was a continuing and cohesive unit with specific and assigned responsibilities and constituted an “enterprise” within the meaning of RICO, 18 U.S.C. § 1961(4).

213. Each RICO Defendant, by engaging in the acts set forth above, participated in the operation and management of the enterprise. At all relevant times, this enterprise was engaged in, and its activities affected, interstate and foreign commerce, within the meaning of RICO, 18 U.S.C. § 1962(c).

214. Each RICO Defendant, by engaging in the acts set forth above, conducted or participated, directly or indirectly, in the conduct of the enterprise’s affairs through a “pattern of racketeering activity” within the meaning of RICO, 18 U.S.C. § 1961(1) and (5), in violation of RICO, 18 U.S.C. § 1962(c), and each participated in a conspiracy to do so in violation of 18 U.S.C. § 1962(d).

215. The RICO Defendants, on numerous occasions, and in furtherance of their scheme to defraud and to obtain money by means of false and fraudulent pretenses, knowingly: (1) repeatedly disseminated information to customers and potential customers through the misappropriated cipherblade.com website, (2) used CipherBlade’s IT infrastructure to leverage those clients and exclude CipherBlade from them, (3) blocked CipherBlade’s rightful access to its IT infrastructure, and (4) profited from the sale through and operation of the misappropriated

CipherBlade website and IT infrastructure in furtherance of Defendants' common financial interest.

216. The RICO Defendants, on multiple occasions and in furtherance of their scheme to defraud, and to obtain money by means of false and fraudulent pretenses, knowingly caused to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, signals, pictures, and sounds, including false and counterfeit pedigrees, in violation of the federal wire fraud statute, 18 U.S.C. § 1343. Each counterfeit pedigree transmitted by wire constituted a separate violation of 18 U.S.C. § 1343 and a separate act of racketeering. The RICO Defendants' use of interstate wire communications to continually upload, transmit, and receive data, information, and communications in furtherance of their unlawful activity, including text messages, mobile phone calls, and emails, was also integral to the scheme and the operation and maintenance of the enterprise.

217. The RICO Defendants, on multiple occasions, and in furtherance of their scheme to defraud and to obtain money by means of false and fraudulent pretenses, knowingly caused to be sent and delivered the misappropriated funds to other RICO Defendants with the intent of concealing the nature, location, source, ownership, and control of the counterfeiting proceeds, in violation of the money laundering statute, 18 U.S.C. § 1956. Each transfer constituted a separate violation of 18 U.S.C. § 1956 and a separate act of racketeering.

218. Each RICO Defendant committed and/or aided and abetted the commission of two or more of these racketeering acts in violation of 18 U.S.C. §§ 2, 1341, 1343, and/or 2320. The RICO Defendants' racketeering acts were multiple and repeated.

219. These multiple racketeering acts were related and constituted a "pattern of racketeering activity" within the meaning of 18 U.S.C. § 1961(5). The acts alleged were related to

each other by virtue of common participants; common victims; a common method of commission; and the common purpose and common result of enriching the RICO Defendants while concealing their unlawful activities.

220. CipherBlade was injured by the RICO Defendants' pattern of racketeering activity because Defendants have taken over business relationships, IT infrastructure, the CipherBlade website, and access to CipherBlade's accounts through this unlawful scheme.

221. As a result of their misconduct, the RICO Defendants are liable to CipherBlade for its injuries.

222. The full scope of the RICO Defendants' fraudulent enterprise is not known, and the RICO Defendants' demonstrated pattern of deceptiveness indicates they may have perpetuated their scheme through unknown entities.

223. Pursuant to 18 U.S.C. § 1964(c), CipherBlade is entitled to recover threefold its damages plus costs and attorneys' fees.

**Predicate Acts of Mail Fraud and Wire Fraud**

224. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs, as if fully set forth herein.

225. The claim for RICO is predicated on other acts. Here, Defendants racketeering activity relied on predicate acts of mail and wire fraud, under 18 USC § 1961.

226. Each RICO Defendant engaged in a pattern of abuse that exceeded authorities granted with the intent to execute their scheme.

227. Defendants engaged in wire fraud when they created an email to impersonate Mr. Sanders and conduct official business on behalf of Plaintiff, in furtherance of their efforts to take control of CipherBlade. This email went so far as to include a photo of Mr. Sanders in the signature

line, giving the impression that he sent the messages from this email address.

228. Defendants also used Mr. Sanders' email to contact customers and business contacts, knowingly using Mr. Sanders' name and photo to induce confusion and make deals to advance their scheme.

229. Defendants engaged in mail fraud when they sent a package from his home, fraudulently using his name, and personal credit card, to an address in Cyprus. This package, upon information and belief, includes relevant documents that belong to the Plaintiff, including the LLC and business filings. These items were mailed with the intention of furthering their scheme, as it included sensitive information about Mr. Sanders' business and was stolen from Mr. Sanders' home.

### **JURY TRIAL DEMANDED**

Pursuant to Fed. R. Civ. P. 35, Plaintiff demands trial by jury as to all issues that may be tried by a jury.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff demand judgment against Defendants and each of them, jointly and severally, as follows:

- 1) Awarding Plaintiff an injunction against Defendants;
- 2) Awarding Plaintiff actual damages for past lost wages and benefits and future lost wages and benefits, in an amount to be determined at trial, but that would be in excess of \$75,000;
- 3) Awarding Plaintiff increased, exemplary and/or treble damages for Defendants intentional tortious conduct;
- 4) Awarding Plaintiff attorneys' fees, costs and treble damages under 18 U.S.C. § 1964(c);



- 5) Awarding Plaintiff the costs of this action together with reasonable attorney's fees;
- 6) Awarding Plaintiff pre- and post-judgment interest in the statutory amount;
- 7) Return of domain cipherblade.com to true CipherBlade;
- 8) Release and return of all IT infrastructure and operations platform (including GSuite) back to CipherBlade;
- 9) Cease onboarding and transferring clients to Defendants, including Alaska and Singapore CipherBlade;
- 10) Prevent Defendants from creating similar CipherBlade organizations in the future in other jurisdictions or using the CipherBlade mark or any mark that is confusingly similar;
- 11) Return of all clients, assets, trade secrets and other confidential information, corporate and business records and monies taken during the takeover of CipherBlade;
- 12) Return the CipherBlade mark to CipherBlade Ltd. and declare its assignment to Defendant Omega3zone Global, and any other assignments or licenses granted by Defendants to be fraudulent, null and void; and
- 13) Such other and further relief as the Court deems equitable, just and proper.

Dated: New York, NY  
July 14, 2023

Respectfully submitted,

*/s/ Alexander Joseph Urbelis*

---

Alexander Joseph Urbelis

Anne Li

James Stronski

Richard J. Stella III

CROWELL & MORING LLP

590 Madison Avenue, 20<sup>th</sup> Floor

New York, NY 10022

Telephone: (212) 223-4000

Fax: (212) 223-4134

Garylene Javier (*pro hac vice pending*)

CROWELL & MORING LLP

1001 Pennsylvania Avenue NW

Washington DC 20004-2595

Telephone: (202) 624-2500

Fax: (202) 628-5116

gjavier@crowell.com

*Attorneys for CipherBlade, LLC, a Pennsylvania  
Limited Liability Corporation.*